AU/AWC/161/1998-04

AIR UNIVERSITY

INFORMATION OPERATIONS: AMERICA'S PLAN FOR STRATEGIC FAILURE

by

Blake F. Lindner, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. George J. Stein

Maxwell Air Force Base, Alabama

April 1998

Disclaimer

The views expressed in this academic research paper are those of the author(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Contents

Page

DISCLAIMER ii

PREFACE iv

ABSTRACT v

INTRODUCTION 1
The Wind of Change 1
The Third Wave: America's Chance to Lead 3

INFORMATION: A STRATEGIC PHENOMENON 6
Why is Information Inherently Strategic? 6
Information Reaches Everyone 6
Worldwide Linkage 7
The Media—Information's Turbocharger 8

AMERICA'S INFORMATION STRATEGY: TWO CRITICAL SHORTFALLS 11
Shortfall #1: The U.S. Military's Operational Approach to Information 11
(1) Joint Vision 2010: An "Operational Template" 12
(2) Battlefield Role of Information Remains Essential 13
(3) Military Reluctance to Accept the Strategic Nature of Information 14
(4) Information Operations Doctrine: Is Change in the Air? 14
Shortfall #2: The Government's Fragmented Information Policy 17
(1) PCCIP: An Insufficient Approach 18
(2) Organizational and Legal Problems—Who Defends American Cyberspace? 20
(3) Strategic Information Operations—How Far Should America Go? 24

RECOMMENDATIONS 36

BIBLIOGRAPHY 39

Preface

This paper addresses shortcomings in the American government's approach to information operations. Specifically, it analyzes two major problem areas—the operationally oriented military approach and the unfocused efforts of the United States government.

My flying experience as an F-4G Wild Weasel, staff experience as an F-117A mission planner, and a joint battlestaff trainer kindled in me a strong interest in the exploitation of information at the tactical and operational levels. At the Air War College, this grew to the strategic-level—the focus of this paper. The research was both captivating and educational although discovering the unresolved issues proved unsettling.

I would like to thank Dr. George J. Stein of the Air War College faculty for acting as my academic advisor, for furthering my interest in the subject, and for leading a truly intriguing elective class on Information Operations. Also, special thanks to Lieutenant Colonel Rakesh N. Dewan for his assistance in exploring concepts and locating research material.

Abstract

This paper highlights problems with America's approach to information operations. These are the military's operational-level fixation and the government's fragmented approach to information operations. The paper recommends leaders fully accept the strategic value of information, include information as an instrument of national power, and broaden the defensive approach of the President's Commission on Critical Infrastructure Protection to include proactive measures.

Chapter 1

Introduction

The Wind of Change

Another summer night;
Soldiers passing by;
Listening to the wind of change…

The wind of change blows straight
Into the face of time,
Like a soft wind
That will ring a freedom bell,
For peace of mind.

—The Scorpions

The Scorpions, a popular German rock band, branded the emotion of the 1989 fall of the Berlin wall into the souls of millions with the above lyrics to their song "Wind of Change."[1] The song punctuated the dramatic conclusion of over four decades of Cold War in which neither side fired a shot! If there was no decisive clash of armed forces, how can Western Europe and the United States claim "victory" over the Warsaw Pact and the former Soviet Union? Was the Cold War really a war? If it was, what were the weapons? What were the targets?

The Cold War was a war of sorts in which the targets were the hearts, the minds, the souls, and the perceptions of the "enemy." Author Carl Builder tells us the walls of the

Cold War were "breached not by military forces, diplomacy, alliances, or economic power, but by information spewing out of television sets, telephones, audio and video tapes, computers, and facsimile machines, into the minds of the individuals."[2]

Clearly, there were pronounced differences in living standards between the West and the East during the Cold War. The imbalance was so large it prompted Zbigniew Brzezinski in his book, The Grand Failure, to predict the fall of the Soviet Union. Specifically, Brzezinski cited huge East-West divergences in per capita GNP, world trade, telephones, motor vehicles, and infant mortality.[3] In addition to others, these factors were significant in setting the stage for the collapse of Russian communism.

Although economics played a central role in the fall of the Soviet Union, information served as the catalyst that brought about that fall. The information flow took many forms. For example, information reached the East European masses through the ceaseless message of Voice of America. Also, Soviet President Mikhail Gorbachev's glasnost campaign of openness unleashed strong impulses for reform in key Soviet urban centers.[4] Both uses of information served to enlighten the masses to the need for change.

The point is this: information used strategically can be effective in precipitating change. The fall of the Soviet Union is one example that proves this. Another was the Vietnam War, a so-called "conflict" in which tactical victories on the battlefield were not enough to overcome a strategic loss of will power among the American people. Likewise, in this instance, the hearts and minds of the opposing populations proved to be more important strategic objectives than any particular piece of ground, any lopsided body count, or any air-to-air kill ratio.

As information continues to fuse the world together into a single global community, American leaders must develop a strategic information policy that promotes democratic principles and American leadership abroad as stated in its national security strategy.

The Third Wave: America's Chance to Lead

> *Knowledge in the form of an informational commodity indispensable to productive power is already, and will continue to be, a major—perhaps the major—stake in the worldwide competition for power. It is conceivable that the nation-states will one day fight for control of information, just as they battled in the past for control over territory, and afterwards for control over access to and exploitation of raw materials and cheap labor.*[5]
>
> —Jean François Lyotard

Few would argue with the idea the world is undergoing an information explosion. Futurist Alvin Toffler describes this fantastic age as history's third major wave of change—the "Third Wave."[6] Characteristics of the Third Wave include a rapid increase in the quantity and speed of transmitting digitized information, a staggering rate of change in information systems and concepts, and questions that befuddle governments and military forces as to how they should "fight for control" of information to achieve their respective ends.

The United States currently has the technological lead in the Third Wave era. In *The American Economy: The Struggle for Supremacy in the 21st Century,* Nicolas Spulber informs us that, in a 1991 review of 94 technologies, the United States was either the leader or was highly competitive in about two-thirds of the technologies considered.[7] These included computer-aided engineering, certain electronic components, a vast number of information-related techniques, and high-level software languages.[8]

The United States must capitalize on its lead in information technologies by formulating a complete strategic approach to information operations that takes advantage of America's strengths and minimizes inherent weaknesses. Now is the time to act.

A poem by Ella Wheeler Wilcox suggests America controls her own fate if she so decides:

> One ship drives East, and another drives West,
> By the self-same gale that blows;
> 'Tis the set of the sail, and not the gale,
> That determines the way she goes.[9]

Wilcox reminds us it is not the environment that determines the ship's direction: it is the tack taken by those at the helm. Likewise, American leadership can choose to succeed or fail at the task of developing an information strategy that affords a fair chance of achieving its stated national security objectives.

While addressing the Air War College Class of 1998 a senior Air Force officer surprised listeners by saying, "The Air Force was never about airborne platforms; it was about fresh thinking!"[10] The speaker was using past tense, but his words may prove to be prophetic. Fresh thinking always precedes adoption of new paradigms. Are American leaders capable of fresh strategic thinking? Can they adopt a paradigm that respects the inherently strategic nature of information? And, do they have the courage to exercise enlightened leadership at the onset of the Third Wave?

Notes

[1] Scorpions, Live Bites Compact Disk #314 526 889-2, Polygram Records, 1995.

[2] Carl H. Builder, The Icarus Syndrome (New Brunswick: Transaction Publishers, 1994), 244-245.

[3] Zbigniew Brzezinski, *The Grand Failure* (New York: Macmillan Publishing Company, 1990), 285-296.

[4] Ibid., 43.

[5] Jean François Lyotard, "The Postmodern Condition: A Report on Knowledge," (1979), quoted in *The Columbia Dictionary of Quotations* on Microsoft Bookshelf 98 Compact Disk, Document no. X03-08963. (Columbia University Press, 1996).

[6] Toffler asserts the First Wave, agricultural civilization, began around 8000 B.C. and lasted until approximately 1650-1750. The Second Wave, industrial civilization, then picked up and lasted until about 1955 in the United States. At that time, white collar and service workers outnumbered blue collar for the first time. Alvin Toffler, *The Third Wave* (New York: Bantam Books, 1980), 14.

[7] Nicolas Spulber, *The American Economy: The Struggle for Supremacy in the 21st Century* (New York: Cambridge University Press, 1995), 64.

[8] Ibid., 64-65.

[9] Ella Wheeler Wilcox, *Bibby's Annual*, quoted in Margaret Thatcher, *The Path to Power* (Great Britain: Harper Collins Publishers, 1995), 7.

[10] Retired Senior U.S.A.F. Officer, Speech to Air War College Class of 1998, Maxwell Air Force Base, Alabama, Fall, 1997.

Chapter 2

Information: A Strategic Phenomenon

In cyberspace, national borders are no longer relevant. Electrons don't stop to show passports.[1]

—President's Commission on Critical Infrastructure Protection

The foundation underlying this thesis is that information is inherently strategic in its nature. As the quote states, information ignores international borders. It is a strategic phenomenon that defies imprisonment; it is widespread, inexpensive, and persistent; it seeks to be free. Any strategy designed to leverage information power must account for its inherently strategic nature.

Why is Information Inherently Strategic?

Information Reaches Everyone

President Reagan once said, "Information is the oxygen of the modern age. It seeps through the walls topped by barbed wire, it wafts across the electrified borders."[2] The former U.S. president had a sixth sense for the unstoppable power of information.

In today's rapidly evolving computer and communications revolution information has indeed taken on strategic significance. This is more true today than previously due to the widespread and still growing electronic interconnectivity provided by radio, television, telephones, fax machines, video teleconferencing, and proliferation of home computers interconnected through the World Wide Web. The growth of computers and communications is reflected in staggering statistics such as increases in American computer industry revenues of over 28% per year since 1965[3] and the tripling of mobile data services (cellular networks, mobile data networks, mobile satellite service, and specialized mobile radio) between 1992 and 1996.[4]

Worldwide Linkage

Walter Wriston, former Chairman and Chief Executive Officer of Citicorp/Citibank and Chairman of the Economic Policy Advisory Board during the Reagan administration, concurs with the widespread nature of the information revolution. Wriston notes:

> We are now living in the midst of the third great revolution in history.... Today, the marriage of computers and telecommunications has ushered in the Information Age, which is as different from the Industrial Age as that period was from the Agricultural Age. Information technology has demolished time and distance. Instead of validating Orwell's vision of Big Brother watching the citizen, the third revolution enables the citizen to watch Big Brother. And so the virus of freedom, for which there is no antidote, is spread by electronic networks to the four corners of the earth.[5]

Clearly, Wriston has captured the strategic essence of information. He believes the convergence of computer and communications technology has caused the world to become a single, global community—a true linkage of rich and poor, north and south, east and west, and city and countryside.[6] Information is the enabler of this linkage. As such, information is the catalyst that has facilitated the re-forming of attitudes and perceptions of the masses, governments, international economics, and militaries; its effects have proven both pervasive and persistent. Information's qualities of pervasiveness and persistence, then, are key elements of its strategic nature.

The Media—Information's Turbocharger

The media have the effect of turbocharging information thereby enhancing its already strategic nature. The largest contributor in this regard is the medium of television, bringing real-time events to living rooms worldwide twenty-four hours a day through as many as seven worldwide competitive networks such as CNN.[7] In this way, the media play a significant role in enhancing the strategic reach of information.

Senior leaders have become painfully aware of the power of the media. They realize real-time dissemination of shocking graphical information gathered from a tactical situation may lead to strategic consequences.[8] For example, the media's ability to almost instantaneously transmit images of death and mutilation can profoundly shape national and international public opinion.[9] Through manipulating public opinion, the media can ignite or constrain government action. For example:

> Beginning with Vietnam, the American public increasingly has had access to video images of U.S. military operations, with a consequent impact on policy. In the days following the introduction of U.S. troops to Haiti in 1994, bloodshed in the streets of Port-au-Prince was broadcast live, leading to immediate White House decisions to redefine the responsibilities of U.S. soldiers to control civil strife.[10]

The danger with the media is that its power is unchecked. If allowed unabated to influence the American or foreign public, the media can become a factor in determining American strategy. This is not necessarily bad; however, there is a danger the media can be a knowing or unwitting accomplice to unfriendly forces thereby influencing American strategy in a negative way. For example, imagine if Hanoi, which conducted an impressive international psychological campaign against the U.S. in Vietnam, had today's information age capabilities at its disposal.[11] The effects of the North Vietnamese information campaign could have been even more dramatic than they actually were. The

Vietnam conflict was a vivid example of the case in which a nation's military can be busy winning operational battles while losing the strategic war in the hearts and minds of the its people in part because of the media.

Alvin Toffler asserts the media have recently undergone de-massification. This de-massification had the effect of breaking up large newspaper, magazine, radio, and television giants of industrial age society. In their place, customized media have sprung up that specifically target the interests of their audiences.[12] Toffler notes this has begun a new era in which a new info-sphere is emerging. This will have the effect on the most important sphere of all, the one inside our skulls.[13] The minds of the populace are therefore susceptible to precision marketing made possible by the de-massified media.

Leaders who fail to understand information is a strategic phenomenon yield the advantage to those who do. The successful governments of tomorrow will be those that formulate information strategies that account for the inherently strategic nature of information.

Notes

[1] President's Commission on Critical Infrastructure Protection, Critical Foundations: Thinking Differently (Washington, D.C.: 1997), 6.

[2] Ronald Reagan, Guardian (14 Jun 1989), quoted in The Columbia Dictionary of Quotations on Microsoft Bookshelf 98 Compact Disk, Document no. X03-08963. (Columbia University Press, 1996).

[3] James E. Person, Jr., ed., Statistical Forecasts of the United States (Detroit: Gale Research Inc., 1993), 66.

[4] Ibid., 67.

[5] Walter B. Wriston, "Bits, Bytes, and Diplomacy," Foreign Affairs, September/October, 1997, 172.

[6] Ibid., 175.

[7] Senior Media Representative, Speech to Air War College Class of 1998, Maxwell Air Force Base, Alabama, Fall, 1997.

[8] Senior U.S. Officer, Speech to Air War College Class of 1998, Maxwell Air Force Base, Alabama, Fall, 1997.

[9] Sidney Bearman, ed., *Strategic Survey: 1995/96* (London: Oxford University Press, 1996), 41.

[10] Robert L. Pfaltzgraff, Jr., and Richard H. Shultz, Jr., eds., *War in the Information Age: New Challenges for U.S. Security* (Washington, D.C.: Brassey's, 1997), 253.

[11] Ibid., 25.

[12] Alvin Toffler, *The Third Wave* (New York: Bantam Books, 1981), 158-165.

[13] Ibid., 165.

Chapter 3

America's Information Strategy: Two Critical Shortfalls

America's information strategy has two major weaknesses. First, the military has been allowed to take an operational approach that focuses on winning battles instead of using information in a broader context to support the political, economic, and information instruments of national power. Second, the national government has not provided a coherent national strategy toward information. At best, national initiatives have been fragmented and uncoordinated.

Shortfall #1: The U.S. Military's Operational Approach to Information

The United States government has allowed the military establishment to develop its own approach to information that emphasizes the operational level of war. Former Chairman of the Joint Chiefs of Staff, General John M. Shalikashvili, spearheaded this approach with his plan for the future—Joint Vision 2010. The following paragraphs briefly discuss four intriguing aspects of the military's approach to the information age. These are (1) Joint Vision 2010's operational-level approach, (2) the still valid, though by itself insufficient, role of operational-level information superiority, (3) the military's reluctance to embrace the strategic aspect of information, and (4) the apparent revolution of emerging doctrine.

(1) Joint Vision 2010: An "Operational Template"

Joint Vision 2010 is not a strategic vision. General Shalikashvili himself dubbed Joint Vision 2010 an "operationally based template."[1] The joint vision is grounded in a conventional, force-on-force concept of the battlespace.[2] The result of this operational approach is that information is a support tool whose objective is creating an interactive "picture" of the battlespace to lessen the fog of war.[3]

As one would well expect, Joint Vision 2010 stands shoulder to shoulder with the national military strategy's operational view of information. Both Joint Vision 2010 and the national military strategy seek to "win the information war" by fusing information to enhance the ability to dominate conventional warfare.[4]

Joint Vision 2010 introduces four emerging concepts to address the uncertain future—dominant maneuver, precision engagement, focused logistics, and full-dimensional protection. These are underwritten by information superiority—something the military sees as a mere technological enabler that allows for achieving desired effects through the tailored application of joint combat power.[5] Information superiority's role is to ensure a successful, cataclysmic clash of conventional armed forces. The implicit, and arguably incorrect, assumption underlying this concept is that tomorrow's conflicts will take the form of a decisive military confrontation between uniformed combatants.

Regrettably, Joint Vision 2010 does not provide a strategic way of thinking about information. Its perspective is purely operational as seen by its belief that "Technological advances will magnify the advantages provided by our high quality force. The promise provided by these technologies is best viewed from an operational perspective."[6]

Senior RAND Corporation analyst Carl H. Builder supports this criticism of Joint Vision 2010. In his article, "Keeping the Strategic Flame," Builder accuses the American military's strategic thinking of going into hiding—Joint Vision 2010 being an example of such thinking. Builder states, "*Joint Vision 2010* is a current illustration of thinking tactically. It is largely about engaging an enemy with joint forces in the future—without evident purpose beyond fighting and winning."[7]

(2) Battlefield Role of Information Remains Essential

The inherently strategic nature of information does not deny its tactical importance on the battlefield. In fact, there are those who believe information is the most important factor on the battlefield. In their book, *War in the Information Age: New Challenges for U.S. Security*, Pfalzgraff and Shultz state, "The present information revolution centers on the concept that the ability to collect, analyze, disseminate, and act upon battlefield information is the dominant factor in warfare."[8] Their view reflects the classical command and control warfare aspect of combat in which the objective is to enhance the military capabilities of friendly forces while reducing the command and control capabilities of the enemy.

But Pfalzgraff and Shultz's view of information is, like Joint Vision 2010, an operational one that presumes an acknowledged state of hostilities between belligerents. Such a view ignores the strategic power of information to diffuse hate propaganda, to spread democratic ideals, and to convince an opponent he has lost the battle before it has begun. No matter how well it is done, command and control warfare on the battlefield is fighting done too late and is capable of achieving only tactical effects.[9]

This paper does not dispute the fact that operational-level information superiority is necessary to achieve victory on the battlefield. In fact, it asserts information dominance on the battlefield is an essential part of a complete strategic approach to information operations. But, in and of itself, General Shalikashvili's vision of information superiority on the battlefield does not constitute a strategic approach to information operations.[10] In other words, battlefield command and control warfare superiority is a necessary but incomplete approach to information operations. It fails to exploit America's current technological superiority at the strategic level. To fully exploit this advantage the military's vision must broaden into the strategic realm. But this will not happen until military leaders accept the inherently strategic nature of information.

(3) Military Reluctance to Accept the Strategic Nature of Information

Today's senior military leaders are familiar and therefore comfortable with the tactical categorization of information. After all, relegating information to a battlefield support role perfectly fits the currently accepted Clausewitzian force-on-force paradigm held dear by numerous American military leaders.

There are problems involving the military's acceptance of the strategic nature of information. Accepting this would require the military to address problems typically outside its span of control and legal authority.

For example, there are problems with involving the military in defending cyberspace because of intractable legal issues such as citizens' rights to privacy as guaranteed by the Fourth Amendment and the law of Posse Comitatus that forbids use of the military to enforce domestic laws. There are also moral and psychological aspects of propaganda campaigns that require more legal authority and expertise than the military has at its disposal. The paper discusses these issues in greater detail in a separate section.

(4) Information Operations Doctrine: Is Change in the Air?

Joint Doctrine. Sanctioned joint doctrine clearly reinforces the operational approach to information—General Shalikashvili's concept of information superiority as a reducer of battlefield uncertainty. But architects of evolving joint doctrine may be sensing the wind of change. An analysis of published and draft doctrine reveals a possible change in old ways of thinking about information.

Traditional thinking is reflected in Joint Pub 3-13.1, *Joint Doctrine for Command and Control Warfare (C2W)*, which was published in February, 1996. This document "focuses on C2W as a part of military strategy for planning or conducting combat at the operational level."[11] Specifically, it states that "command and control warfare (C2W) is an application of IW in military operations and employs various techniques and technologies to attack or protect a specific target set—command and control (C2)."[12] This view fits the classic notion that command and control is simply a military target like any other on the battlefield. Those targets are susceptible to attack and these attacks are called information warfare or command and control warfare. This traditional way of categorizing C2W fits old paradigms perfectly. Perhaps this fact accounts for JP 3-13.1's approval and publication almost two years ago. The JP 3-13.1 notion of C2W is joint doctrine's accepted, operationally based view of information.

But a new, more radical and strategically oriented mindset may be emerging. Joint Pub (JP) 3-13, *Joint Doctrine for Information Operations*, has yet to be published although the draft version is now undergoing coordination. Draft JP 3-13 is a bold attempt to alter the force-on-force paradigm by elevating the importance of information operations to a level commensurate with the strategic importance of information as described in the previous chapter. Specifically, it acknowledges a role for information operations at the strategic level of war. It also recognizes the need to conduct information operations during peacetime as well as during war.[13]

The following excerpts indicate a non-traditional way of thinking about information operations (IO):

> Offensive IO may be the main or supporting effort of a JFC's [Joint Force Commander's] campaign or operation, or a phase of these.[14]
>
> IO can help deter adversaries from initiating actions detrimental to the interests of the United States or its allies/coalition partners.[15]

These quotations reflect thinking far beyond traditional approaches to information. It is revolutionary to suggest that information operations may be the main effort and they can deter conflict. These ideas should raise eyebrows among Clausewitz's followers and smiles among Sun Tzu's. After all, the idea of bloodshed was central to the theories of Clausewitz.[16] On the contrary, Sun Tzu advised us, "Those skilled in war subdue the enemy's army without battle."[17] Are today's leaders on the verge of changing?

It will be interesting to see if the draft joint doctrine obtains approval without substantive change. After all, the draft JP 3-13 is driving a wedge between old doctrine and new; between operational and strategic thinking; between the ideas of "information in war" and "information warfare"; between Clausewitz and Sun Tzu. Joint doctrine is not alone in attempting to change the information paradigm; Air Force doctrine is apparently steering the same course.

Air Force Doctrine. Draft Air Force doctrine is also introducing a new approach to information. Like its joint counterpart, Air Force Doctrine Document (AFDD) 2-5, *Information Operations* (4th draft) addresses information with a non-traditional perspective. For example, it headlines former Air Force Chief of Staff General Ronald Fogleman's concept of the information battlespace as a fifth dimension—one beyond the traditional realms of air, land, sea, and space.[18] It recognizes that information has progressed from an adjunct to weapons to being widely recognized as a weapon or target itself.[19] It also introduces the strategic, and somewhat radical, notion of information in support of the "boundless battle."

> War in the future is unlikely to be bounded by the geographical restrictions of terrain and distance. This "boundless battle" includes continual nonlethal combat prior to the application of traditional military force (if any). One intent of the "boundless battle" is to achieve objectives with limited normal force applications or possibly averting normal force application altogether. The "boundless battle" will, in all likelihood, incorporate economic and political "combat" using information and information technology to employ the economic and political instruments of national power in a coordinated and effective manner.[20]

If AFDD 2-5 and JP 3-13 obtain approval without substantive changes, they will spearhead a significant shift in the traditional military way of thinking about information.

Toffler has also noted this shift in doctrinal paradigms. He observes a strategic shift in doctrinal thinking by the Joint Chiefs of Staff, the National Defense University, West Point, the Analytic Science Corporation (a private think tank), and other intellectuals. The new concepts are going beyond the operational realm into the strategic by introducing information as a "strategic asset" that can alter high-level decisions of the opponent and actually deliver a knockout punch before the outbreak of traditional hostilities.[21]

Shortfall #2: The Government's Fragmented Information Policy

The popular author of *Information Warfare*, Winn Schwartau, offers a national information policy for consideration.[22] Schwartau's suggestion of a national policy underscores the fact America has no recognizable overarching information strategy. At best, the American government has undertaken piecemeal efforts that have resulted in a fragmented and problem-ridden information policy. Captain Stephen A. Rose, a Navy Judge Advocate General, describes this approach using the analogy of a "car with a good engine, a bad transmission, three steering wheels and no road map."[23] We will analyze three key problem areas of the government's approach. These are: (1) the President's Commission on Critical Infrastructure Protection (PCCIP), (2) unresolved organizational and legal issues, and (3) the unclear role of strategic information operations.

(1) PCCIP: An Insufficient Approach.

The PCCIP does not offer a complete strategic approach to information for three reasons. First, it addresses only defensive issues. Second, it addresses only tactical-level threats. Third, its recommendations are designed to insure the integrity of the communication network that is exploitable by unfriendly actors at the strategic level. We shall discuss these inadequacies after reviewing some background information on the PCCIP.

Background. The President's Commission on Critical Infrastructure Protection was formed in 1996 amid rumors of a possible electronic Pearl Harbor. President Clinton appointed the commission by executive order and tasked it to propose a national policy for protection and assurance of the nation's critical national infrastructures.[24] The commission was comprised of representatives from federal departments and agencies as well as the private sector. It also had a designated team that addressed information and communications concerns.[25]

The commission did its job well. It produced an enlightening study that revealed an increasing national dependence on electrical energy, communications, and computers. It also uncovered vulnerabilities to physical attack, cyber threats, recreational hackers, criminal activity, terrorism, and information warfare.[26] The study made numerous recommendations as to how these vulnerabilities can be minimized. But the study fell short of satisfying the requirement for a national information strategy for three reasons.

A Defensive Approach. Because the PCCIP addresses only defensive issues it does not constitute a complete information strategy. The President's executive order empowered the commission only to identify infrastructure vulnerabilities and recommend possible solutions to them. There was no tasking or authority to investigate offensive uses of information in any way.[27]

A Tactical-Level Approach. The PCCIP dealt only with physical and cyber threats at the tactical level. Specifically, it addressed physical threats such as dynamite or fertilizer bomb attacks as well as cyber attacks made probable by a growing computer-literate population, adoption of common public protocols that have increased system interconnection, and "hacker tool" libraries.[28]

The study was not tasked to address strategic issues such as the vulnerability of the American public to deliberate misinformation campaigns executed through the American communications infrastructure. The web, for example, can and is used for niche marketing by various businesses. It can as easily be used as a means to disseminate hate propaganda or other dangerous and uncensored messages specifically targeted at vulnerable interest groups. The PCCIP did not investigate strategic vulnerabilities, only tactical ones.

The PCCIP Insures the Availability of the Communications Network for Unfriendly Actors. An unavoidable, but detrimental, side-effect of the PCCIP is that its recommendations seek to insure the integrity of a communications infrastructure that can be used by groups hostile to the United States. By insuring the integrity of America's communication networks, unfriendly actors with hostile intent are guaranteed direct access to the nation's strategic center of gravity—the minds of the American people. Thus, hostile nation-states and ill-intentioned extremist groups are empowered via their assured access to the world's most interconnected public.[29] Ironically, they have the cooperative effort of the American government and industry to thank for providing it to them.

The web is not only a potential information weapon; it can support physical attacks as well. For example, the commission's report points out information readily available on the web may disclose to a terrorist the best place to set explosive charges for maximum disruptive effect.[30]

(2) Organizational and Legal Problems—Who Defends American Cyberspace?

There are troublesome organizational and legal problems standing in the way of a workable national information operations policy. Organizational and legal issues are so closely intertwined it is logical to discuss them together. The heart of the issue centers on the question of who should be responsible for defending America's information infrastructure.

Opinions vary as to where that responsibility lies. Should it be the U.S. military, the civil sector, or a government agency like the Central Intelligence Agency (CIA), the Federal Bureau of Investigation (FBI), or the Department of Justice (DOJ)?

The Military. First, consider the military. The military has several tools that seem to make it the logical choice to defend our nation's infrastructure including cyberspace. These include the pillars of defensive information operations namely information assurance, physical security, operations security, counter-deception, counterpsychological operations, electronic protection, and special information operations.[31] The military also has robust intelligence assets, such as monitoring capabilities, that support these measures.[32] It also has highly trained and experienced personnel. The capabilities of the military seem to make it a perfect match for the task. This is the opinion of author Winn Schwartau who feels it is the most appropriate organization for the job.[33]

Unfortunately, there are legal problems with assigning the military the task of defending cyberspace. The Air Force's *Cornerstones of Information Warfare* points out one of these:

> There is a troubling offense-defense asymmetry in the scope of information warfare. The military may, consistent with the law of armed conflict, attack any militarily significant target. In the context of information warfare, this means we may target any of the adversary's information functions that have a bearing on his will or capability to fight. In stark contrast, our military may defend only military information functions. There are many information functions critical to our national security that lie outside the military's defensive purview.[34]

This restriction to military jurisdiction is grounded in the Posse Comitatus law of 1878. Posse Comitatus forbids the military from operating within the U.S. borders without specific authorization.[35] The military, therefore, cannot be assigned the mission of defending the nation's information infrastructure unless the law is amended.

The Civil Sector. Second, the President's Committee on Critical Infrastructure Protection implied the civil sector plays a role in providing the defense of the national information infrastructure. Its study alarmingly states the owners and operators of our critical infrastructures are now on the front lines of the nation's security efforts![36] The Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, Emmett Paige, Jr., concurs. Paige has voiced the need for an information policy that incorporates civil agencies at all levels and the commercial sector to insure information protection from internet intrusion.[37]

The suggestion American civilians play a role in the defense of the nation's infrastructures without legal empowerment, authority, or funding is alarming to say the least. The commission's recommendation of "cooperation and information sharing" based on partnerships among the infrastructure owners and government agencies is a hopeful, but unworkable, proposal. It ignores conflict of interest problems and contentious legal issues involved in the defense of American cyberspace. [38]

The government must put forth a realistic plan that is sensitive to conflict of interest problems regarding the civil sector's aversion to sharing information concerning security matters. An illustrative example is the banking industry which is reluctant to report electronic vulnerabilities because the potential public relations fallout is too great.[39]

There are problems in assigning tasks and responsibilities for the civil sector because they are not legally enforceable. The idea of government and civil information sharing is noble, but it cannot succeed on good will alone. It can not be assumed civil authorities will feel comfortable relinquishing information, particularly regarding their own vulnerabilities, to the government for fear of leaks or abuse. The government may have to institute laws mandating sharing of information regarding information system weaknesses.

A Government Agency—CIA, FBI, or DOJ. Third, why shouldn't a government agency such as the Central Intelligence Agency, the Federal Bureau of

Investigation, or the Department of Justice be responsible for defense of the national infrastructure? Unfortunately, there are constitutional problems with this idea.

In "Bits, Bytes, and Diplomacy," Walter Wriston informs us, "The bureaucratic distinctions between intelligence and law enforcement, between permitted surveillance at home and abroad, may be unsuited for information warfare. There are no borders in cyberspace to mandate these distinctions."[40] Wriston also points out the dilemma of working to resolve legal responsibilities in the areas between the First Amendment and national security, and the right to privacy through encryption and the National Security Agency's desire to breach it.[41]

Constitutional restrictions therefore make it difficult to assign perfectly distinct organizational responsibilities between government agencies in the Information Age. This was intentional, not accidental. Years ago, the framers of the constitution purposely separated certain legal authorities to allow for checks and balances among the three branches of government. Consequently, the authority of government agencies to collect and disseminate information was intentionally "stovepiped" by legal statute, executive order, or regulation.[42]

A phenomenon of cyber attacks that adds to the interagency problem is the difficulty in determining who is making the attack. The inherent anonymity makes for a wrenching legal problem as to who is empowered to investigate. The PCCIP report confirms this by stating, "With the existing rules, you may have to solve the crime before you can decide who has the authority to investigate it."[43] Under yesterday's laws, government agencies can not effectively provide for the surety of the nation's information infrastructure.

The consequences of not resolving which organization or organizations are responsible for the nation's cyber defense are serious. America's national security, global economic competitiveness, and domestic well being are at stake.[44]

(3) Strategic Information Operations—How Far Should America Go?

America has no clear policy that clarifies how far it will go in using strategic information operations to achieve its goals. By strategic information operations, we are referring to the idea of psychological operations applied on a strategic scale through the full array of modern communications channels including the internet. Psychological operations are defined as "operations planned to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals.[45]

In other words, the information revolution is overtaking the world, the internet is growing rapidly—already a system of 70,000 networks—and nobody knows if or how U.S. leaders are going to use its information advantage in a strategic way to implement the national strategy of engagement. The U.S. government is not taking a proactive stance in this regard. Instead, it is choosing to address national security objectives through more conventional means such as diplomacy and economics.

There are reasons for and against developing a clear policy regarding strategic information operations. Unfortunately, American leadership has not exercised its leadership in stating to what degree the nation will use its information edge in pursuing national policies and in what way this will be accomplished.

Reasons For Supporting Strategic Information Operations. There are three sound reasons for aggressively pursuing information operations at the strategic level. These are that the U.S. has agencies already in place with a history of substantial success, the U.S. has an exploitable information advantage, and strategic uses of information can enhance America's other instruments of national power.

First, the United States already has organizations that have a solid start in getting its strategic message out. Examples are the U.S. Information Agency (USIA) and its broadcasting arm, the Voice of America. Both of these have histories that include success stories. Joseph S. Nye, Jr., and William A. Owens point out:

> USIA's international broadcasting arm, the Voice of America, has in the last few years become the primary news source for 60 percent of the educated Chinese.[46]

The U.S. military services also have substantial psychological operations capabilities including experienced organizations and refined doctrinal procedures.[47]

Second, the U.S. currently enjoys an advantage in information technologies that can be put to effective use. The U.S. edge stems from its ability to collect, process, act upon, and disseminate information. This edge is likely to grow in the next decade.[48] Nye and Owens suggest this information advantage can be put to use in various ways. These include aiding democratic transitions in the remaining communist and authoritarian states, promoting democracies, preventing and resolving regional conflicts, addressing terrorist threats, international crime, proliferation of weapons of mass destruction, and damage to the environment.[49] They also note, "America's increasing technical ability to communicate with the public in foreign countries, literally over the heads of their rulers via satellite, provides a great opportunity to foster democracy. It is ironic to find Congress debating whether to dismantle USIA just when its potential is greatly expanding."[50] Clearly, Nye and Owens are keenly aware of the strategic nature of information and how America can leverage its capabilities at the strategic level.

Colonel Frank L. Goldstein recommends a similar strategic use of information programs. Goldstein feels information programs should disassociate terrorist groups from pockets of support, publicly impugn the worth of terrorist objectives, and denigrate their leadership.[51]

Third, Nye and Owens believe information can be used to enhance the concept of soft power. Soft power is the idea that nations can be influenced through attraction rather than coercion.[52] Information, they feel, is a force multiplier that assists diplomatic and economic efforts. [53] Using information to enhance the effectiveness of soft power can, in this way, provide an effective, non-military option to achieving national objectives.

Reasons Against Use of Strategic Information Operations. There are also reasons against the use of information as a strategic tool. These include problems in determining a single national message, an inherent American aversion to performing psychological operations during peacetime, problems in interagency coordination, and the fact that government is not the only entity involved in executing strategic information operations.

First, it is becoming increasingly difficult to determine a single national "truth" to put forth. Carl H. Builder in his book, *The Icarus Syndrome*, notes power has shifted from governing elites to individuals within the state as a result of information technologies. This shift is rendering impotent the traditional powers of the state—political, economic, and military.[54] Similarly, Michael Moynihan points out that new technologies have enabled products and messages to be custom tailored for specific audiences. This has eroded any single entity's ability to control information. He observes this "narrowcasting" has multiplexed America's view of the truth.[55] Technology's empowerment of the citizenry has therefore created multiple versions of the truth thereby complicating the government's ability to put forth a single, strategic American message.

Second, the United States is uncomfortable with the use of psychological operations especially during peacetime. Psychological operations expert Colonel Frank L. Goldstein informs us psychological operations have never been accepted by the executive, the Congress, or the American people except in times of war, namely World War I and World War II."[56]

Third, Navy Judge Advocate, Captain Stephen Rose, indicated the Achilles' heel of information operations is the unrelenting interagency coordination process.[57] Dr. Daniel Kuehl of the National Defense University makes the same point regarding the difficulties of coordinating strategic information operations among separate government agencies:

> Strategic information operations thus differ from military information warfare in two important ways: IO spans the conflict spectrum from peace to war and back to peace, and it involves all elements of the national government, not solely the military. These are important considerations precisely because the effort and coordination needed to engage the entire panoply of government organs is a particularly difficult and sensitive affair.[58]

Thus, the inherent difficulties of the interagency process serve as negative factors making strategic information operations a difficult option to plan and execute.

Fourth, employing information in a strategic way involves more than just the government. This is because the strategic use of information involves the art of statecraft in integrating economic, military, diplomatic, technological, and other forms of national power, including civilian information capabilities.[59] The fact strategic information operations involve engaging certain civilian capabilities may serve as a restraining force in the decision to use them.

Strategic Information Operations: Afterthoughts. The question of strategic information operations directly involves the heart of the national psyche. Do all Americans feel justified in asserting their collective national beliefs onto other people? The government has been amazingly successful at circumventing the issue. On one hand, the government proclaims a national strategy of engagement with a goal of spreading democracy. Yet it fails to state how information will be used proactively to facilitate this strategy.

The factors that favor or oppose the use of information operations at the strategic level influence where government leaders stand on the continuum of possible strategic approaches. At one end of the continuum is minimal use—cyber isolationism. At the other end lies netwar—a societal-level ideational conflict waged in part through internetted modes of communication.[60] In other words, at one end is a policy of reticence, the other psychological dominance.[61]

Cyber isolationism is not possible. If the American government elects not to act, the international communication already occurring between information-empowered citizens will carry the collage of America's "message" as told by millions of citizens espousing different versions of the truth. The message gets out; the government just doesn't get a vote in what the message says. An attempted policy of cyber isolationism by the government is therefore ineffective; citizens at their computers will carry the day. Thus, information isolation is not even possible in the Information Age.

At the other extreme lies netwar. Some individuals espouse netwar as a viable strategic information option. For example, Lieutenant Commander William M. Luoma advocates netwar as a suitable alternative to force particularly for operations other than war.[62] Another strongly proactive approach on this end of the continuum is that by Charles Swett, who in his article "Strategic Assessment: The Internet," proposes use of the internet as an appropriate medium for conducting psychological operations.[63] Yet another is Toffler's concept of anti-war that espouses the strategic applications of military, economic, and informational power to reduce the violence so often associated with change on the world stage.[64]

So, the question remains "How far should America go?" Asking such a question is akin to asking a master chef, "How much spice is right?" or a Picasso, "How does one paint a masterpiece?" The mere questions imply there exists a Jominian response as if there were a single, specific, quantifiable, and therefore "correct" response. Unfortunately, the answer is not so simple.

The personalities of top leaders can be instrumental in determining where the national approach lies on the continuum. Certain charismatic leaders personify and voice the nation's strategic message well. Presidents Kennedy and Reagan were such inspirational leaders. Under strong leadership the apparatus that amplifies the national strategic message would likely survive criticism because of relatively stable public support. This would enable a move toward the more assertive end of the continuum.

Other leaders may not have the stage presence or popularity to voice an accepted national stance. In this instance, a national strategic information capability, no matter how efficient the equipment and organizations, would weaken under criticism. The strategic information operation could even backfire as a politically devious American propaganda campaign. Those familiar with psychological operations and public affairs operations are painfully aware of historical examples that have undermined the credibility of such capabilities. That is why psychological operations are first and foremost truth projection activities.[65]

Because top leaders have not formulated a clear national information policy various parts of the government and the civil sector have taken different tacks. Examples of this are the draft joint and Air Force doctrine documents discussed earlier. These documents are sliding to the more activist end of the continuum. The civil sector is going in countless directions as Third Wave de-massification becomes increasingly widespread. The number of web sites is rapidly increasing, each espousing its own customized viewpoint. The way the world communicates today is driven more by people like Bill Gates than governments. Some experts argue the international communications technology is causing the very erosion of the nation-state system.[66]

The national security strategy fails to mention strategic or any other use of information as an instrument of power. This is ironic in a document that emphasizes the "imperative of engagement."[67] Instead, it refers to traditional tools such as diplomacy, monetary assistance, arms control, nonproliferation initiatives, and military activities such as forward stationing and deployment of forces, exercises, and nuclear deterrence.[68] The only reference to information at all is a single, three-sentence paragraph stating the nation must protect its information infrastructure. This is an obvious reference to the President's Committee on Critical Infrastructure Protection. The PCCIP was discussed earlier where it was shown the PCCIP does not offer an adequate national information strategy.

In summary, regarding strategic information operations, the government has taken a position by *not* taking a position. The result is a disconcerting fragmentation of effort. The U.S. military is developing information operations doctrine that is at best superfluous to the national security strategy and at worst in conflict with it. The civil sector is proceeding in disparate directions motivated by the profit motive. The legal and judicial systems eschew fundamental legal and constitutional issues. The lack of government guidance has therefore resulted in disjointed efforts by the nation's military, civilian, legal, and judicial entities.

Notes

[1] Joint Chiefs of Staff, Joint Vision 2010 (Washington, D.C.) Introduction.

[2] The joint definition describes the battlespace as the air, land, sea, and space and the included enemy and friendly forces, facilities, weather, terrain and the electromagnetic spectrum within the area of influence and area of interest. The Joint Staff, *Concept for Future Joint Operations: Part II—Terms and Definitions* on Joint Electronic Library Compact Disk, (Washington, D.C.: GPO, 1997), s.v. "battlespace."

[3] The Joint Chiefs of Staff, *Joint Vision 2010* (Washington, D.C.), 13.

[4] Joint Chiefs of Staff, *National Military Strategy of the United States of America 1995* on Joint Electronic Library Compact Disk, (Washington, D.C.: GPO, 1997), 15.

[5] Ibid., 17.

[6] Ibid.

[7] Carl H. Builder, "Keeping the Strategic Flame," *Joint Force Quarterly* (Winter 1996-97): 76-84, quoted in *Readings for Future Conflict Studies*. (Montgomery: Air University, 1997), 208.

[8] Robert L. Pfaltzgraff, Jr., and Richard H. Shultz, Jr., eds., *War in the Information Age: New Challenges for U.S. Security* (Washington, D.C.: Brassey's, 1997, x.

[9] Richard Szafranski, "An Information Warfare SIIOP," quoted in Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1996), 118.

[10] The Air Force defines information operations as any action involving the acquisition, transmission, storage, or transformation of information that enhances the employment of military forces. Department of the Air Force, *Cornerstones of Information Warfare* (Washington, D.C.), 11.

[11] *Joint Chiefs of Staff, Joint Pub 3-13.1: Joint Doctrine for Command and Control Warfare (C2W)* (Washington, D.C.: 7 February 1996), i.

[12] Ibid., v.

[13] Joint Chiefs of Staff, *Joint Pub 3-13: Joint Doctrine for Information Operations*, 2nd Draft (Washington, D.C.: 2 July 1997), I-1 - I-3.

[14] Ibid., II-3.

[15] Ibid., I-7.

[16] Michael Handel, *Masters of War: Sun Tzu: Clausewitz and Jomini* (Undated), 1-31, quoted in Capt Juile Catt, Audrey Danziger, Lt Col Edward G. Holland, Dr Thomas Hughes, eds., *Strategy, Doctrine and Air Power: Book I* (Maxwell Air Force Base: Air University Press, Undated), 139.

[17] Sun Tzu, *The Art of War*, trans. Samuel B. Griffith (New York: Oxford University Press, 1971), 79.

[18] Department of the Air Force, *Air Force Doctrine Document 2-5: Information Operations*, 4th Draft (Washington, D.C.: 22 July 1997), 1.

[19] Ibid., 3.

[20] Ibid.

[21] Alvin Toffler and Heidi Toffler, *War and Anti-War: Making Sense of Today's Global Chaos* (New York: Warner Books, Inc., 1995), 164-165.

[22] Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1996), 636-647.

[23] Stephen A. Rose (Capt, U.S. Navy), "Information Operations in Joint/Coalition Operations," briefing for "Legal Aspects of Information Operations Symposium," Maxwell Air Force Base, 20-22 October 1997.

[24] These include telecommunications, electrical power systems, gas and oil production, storage, and transportation, banking and financial institutions, transportation, water supply systems, emergency services, and government services. President's Commission on Critical Infrastructure Protection, *Our Nation's Critical Infrastructures: Working Definitions*, 1997, n.p.; on-line, internet, 10/6/1997, http://www.pccip.gov/glossary.html.

[25] The Information and Communications Sector Team addressed the areas of telecommunications, internet, computers, software, fiber optics, and satellites. President's Commission on Critical Infrastructure Protection, *Overview Briefing*, June 1997, n.p.: on-line, internet, http://www.pccip.gov, 6.

[26] The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Thinking Differently* (Washington, D.C.: Undated), 3-5, on-line, internet http://www.pccip.gov.

[27] President, Executive Order 13010, "Critical Infrastructure Protection, amended by EO 13025, 13041, and 13064" (15 July 1996), 1-5, on-line, internet www.pccip.gov/eo13010.html.

[28] The President's Commission on Critical Infrastructure Protection, *Critical Foundations: Thinking Differently* (Washington, D.C.: Undated), 3, on-line, internet http://www.pccip.gov.

[29] Close to half of all computer capacity and 60 percent of internet assets reside in the US. President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Oct 1997* (Washington, D.C.: October, 1997), 4, on-line, internet http://www.pccip.gov.

[30] Ibid., 5.

[31] Joint Chiefs of Staff, *Joint Pub 3-13: Joint Doctrine for Information Operations*, 2nd Draft (Washington, D.C.: 2 July 1997), GL-9.

[32] Joint Chiefs of Staff, *Joint Pub 3-13.1: Joint Doctrine for Command and Control Warfare (C2W)* (Washington, D.C.: 7 February 1996), III-1 - III-2.

[33] Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1996), 47.

[34] *Department of the Air Force, Cornerstones of Information Warfare,* 3.

[35] United States Statutes at Large, Chapter 263, Sec. 15 (June 18, 1878): quoted in Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1996), 47.

[36] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Oct 1997 (Washington, D.C.: October, 1997), vii, on-line, internet http://www.pccip.gov.*

[37] "Information Warfare Strings Trip Wire Warning Strategy," Signal (Undated): 11.

[38] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Oct 1997* (Washington, D.C.: October, 1997), xi, on-line, internet http://www.pccip.gov.

[39] Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1996), 105.

[40] Walter B. Wriston, "Bits, Bytes, and Diplomacy," *Foreign Affairs*, September/October, 1997, 179-180.

[41] Ibid., 180.

[42] President's Commission on Critical Infrastructure Protection, *Overview Briefing* (Washington, D.C.: June, 1997), 19, on-line, internet http://www.pccip.gov.

[43] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Thinking Differently* (Washington, D.C.: 1997), 6.

[44] President's Commission on Critical Infrastructure Protection, *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Oct 1997* (Washington, D.C.: October, 1997), vii, on-line, internet http://www.pccip.gov.

[45] Joint Chiefs of Staff, *Joint Pub 3-53: Doctrine for Joint Psychological Operations* (Washington, D.C.: 10 July 1996), v.

[46] Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs* (March/April 1996): 20-36, quoted in *Readings for Future Conflict Studies*. (Montgomery: Air University Press, 1997), 338.

[47] JP 3-53 describes joint PSYOPS policies, procedures, and organizations.

[48] Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs* (March/April 1996): 20-36, quoted in *Readings for Future Conflict Studies*. (Montgomery: Air University Press, 1997), 328.

[49] Ibid., 338.

[50] Ibid.

[51] Frank L. Goldstein, *Psychological Operations: Principles and Case Studies* (Maxwell Air Force Base, Alabama: Air University Press, 1996), 19.

[52] Joseph S. Nye, Jr., and William A. Owens, "America's Information Edge," *Foreign Affairs* (March/April 1996): 20-36, quoted in *Readings for Future Conflict Studies*. (Montgomery: Air University Press, 1997), 329.

[53] Ibid., 328-330.

[54] Carl H. Builder, *The Icarus Syndrome* (New Brunswick: Transaction Publishers, 1994), 239-240.

[55] Michael Moynihan, *The Coming American Renaissance* (New York: Simon and Schuster, 1996), 224.

[56] Frank L. Goldstein, *Psychological Operations: Principles and Case Studies* (Maxwell Air Force Base, Alabama: Air University Press, 1996), 321.

[57] Stephen A. Rose (Capt, U.S. Navy), "Information Operations in Joint/Coalition Operations," briefing for "Legal Aspects of Information Operations Symposium," Maxwell Air Force Base, 20-22 October 1997.

[58] Daniel Kuehl, "Defining Information Power," *Institute for National Strategic Studies-Strategic Forum* 115 (June 1997): 3.

[59] Ibid.

[60] John Arquilla and David Ronfeldt, "Cyberwar is Coming!" *Comparative Strategy* 12 (April-June, 1993): 141-165, quoted in George J. Stein, "Information War—Cyberwar—Netwar," *Readings for Future Conflict Studies* (Montgomery: Air University Press, 1997), 346.

[61] Psychological dominance means the ability to destroy, defeat, and neuter the will of an adversary to resist; or convince the adversary to accept our terms and aims short of using force. The target is the adversary's will, perception, and understanding. Harlan Ullman and James Wade, Jr., *Shock and Awe* (Washington, D.C.: GPO, 1996), 11.

[62] William M. Luoma (Lt Cdr), "Netwar: The Other Side of Information Warfare," Naval War College Research Paper, 8 February, 1994, Defense Technical Information Center, Alexandria, VA., ii.

[63] Winn Schwartau, *Information Warfare* (New York: Thunder's Mouth Press, 1996), 93.

[64] Alvin Toffler and Heidi Toffler, *War and Anti-War: Making Sense of Today's Global Chaos* (New York: Warner Books, 1995), 3.

[65] Joint Chiefs of Staff, *Joint Pub 3-53: Doctrine for Joint Psychological Operations* (Washington, D.C., 10 July 1996), vi.

[66] Carl H. Builder, *The Icarus Syndrome* (New Brunswick: Transaction Publishers, 1994), 239.

[67] President of the United States, *A National Security Strategy for a New Century* (Washington, D.C., 1997), 2.

[68] Ibid., 6-8.

Chapter 4

Recommendations

The American government's failure to formulate and implement a cohesive national approach to information operations is a plan for strategic failure. Leadership must do three things to turn this around. It must leverage the inherent power of information, emphasize strategic-level (vice operational-level) capabilities of military information operations, and confront organizational and legal issues. Fortunately, the nation is like the ship whose direction is determined by the captain at the helm not the wind's direction. Thus, strong leadership can seize the initiative and set the nation on a course for success if it so chooses.

Several recommendations logically follow this paper's identification of various U.S. government and military failures. These are: (1) top leaders appreciate the inherently strategic nature and power of information, (2) revision of the national security strategy to include use of information as an instrument of national power, and (3) a broadening of the national information strategy to include proactive uses of information.

The first recommendation is a change in attitude. Top government and military leaders must come to understand information is a strategic commodity powerful enough to generate wealth, be the object and method of fighting war, and touch everyone thereby changing roles of citizens and governments. The military in particular must understand the difference between *information in war* and *information warfare.* The former is a relegation of information to a support role for conventional combat; the latter is a strategic use of information to affect human perceptions on a broad scale. This shift in thinking does not obviate the need for successful information in war. It simply adds the strategic dimension of information.

The change in military thinking required is from Clausewitzian-style conventional battles to the Sun Tzu approach that pits mind against mind thereby emphasizing the psychological aspect. Along with this paradigm shift is the change in thinking from the Industrial Age to the Information Age. The former held *information supports force;* the latter that *force supports information.*

The change in thinking will also require changes in officer recruitment, the professional military education system, and non-commissioned officer career management. The industrial era recruitment of scores of engineers thinking in terms of mass production to support a Cold War strategy of attrition must give way to recruitment of a different kind of officer. Officers of the future must be historians, political scientists, regional experts, and, in a way, diplomats that understand the subtle power involved in knowing and appreciating a nation's language and culture. Assignments should focus on developing officers as European, Pacific, South American, or Asian experts and emphasize reassignment to their regions of expertise. Also, the non-commissioned officer corps can no longer be mass numbers of soldiers that comprise armies of attrition; they must be the world's most highly trained experts capable of handling the unpredictable demands of situations such as sensitive peacekeeping operations in front of CNN cameras.

Second, the national security strategy must grow to incorporate information as an essential strategic element of national policy. The lack of such mention highlights a conflict between a strategy of engagement and a fragmented approach to strategic information operations that fails to support that strategy.

Third, the President's Commission on Critical Infrastructure Protection work was a good effort, but it fell short of providing the proactive dimension of a complete information strategy. The national strategy must clearly state how the current American advantage in information technologies will be leveraged. This is the most critical factor in establishing a coherent national plan for effective use of information at the strategic level.

Bibliography

Arquilla, John and David Ronfeldt. "Cyberwar is Coming!" *Comparative Strategy* 12 (April-June, 1993). Quoted in George J. Stein. "Information War—Cyberwar—Netwar." *Readings for Future Conflict Studies*, 345-353. Montgomery: Air University Press, 1997.

Bearman, Sidney, ed. *Strategic Survey: 1995/96.* London: Oxford University Press, 1996.

Builder, Carl H. *The Icarus Syndrome*. New Brunswick: Transaction Publishers, 1994.

Brzezinski, Zbigniew. *The Grand Failure*. New York: Macmillan Publishing Company, 1990.

Goldstein, Frank L. *Psychological Operations: Principles and Case Studies*. Maxwell Air Force Base, Alabama: Air University Press, 1996.

Handel, Michael. *Masters of War: Sun Tzu: Clausewitz and Jomini*. In *Strategy, Doctrine and Air Power: Book I*, ed. Capt Juile Catt, Audrey Danziger, Lt Col Edward G. Holland, and Dr Thomas Hughes, 133-192. Maxwell Air Force Base: Air University Press, Undated), Undated.

Kuehl, Daniel. "Defining Information Power." *Institute for National Strategic Studies-Strategic Forum* 115 (June 1997).

Luoma, William M. "Netwar: The Other Side of Information Warfare." Defense Technical Information Center, Alexandria, VA, 1994.

Lyotard, Jean François. *The Postmodern Condition: A Report on Knowledge*. (1979). Quoted in *The Columbia Dictionary of Quotations*, on Microsoft Bookshelf 98 Compact Disk, Document no. X03-08963. Columbia University Press, 1996.

Moynihan, Michael. *The Coming American Renaissance: How to Benefit from America's Economic Resurgence*. New York: Simon and Schuster, 1996.

Nye, Joseph S., Jr., and William A. Owens. "America's Information Edge." *Foreign Affairs*. (March/April 1996). 20-36. Quoted in *Readings for Future Conflict Studies*, 328-344. Montgomery: Air University Press, 1997.

Person, James E., Jr., ed. *Statistical Forecasts of the United States*. Detroit: Gale Research, Inc., 1993.

Pfaltzgraff, Robert L., Jr., and Richard H. Schultz, Jr., eds. *War in the Information Age: New Challenges for U.S. Security*. Washington, D.C.: Brassey's, 1997.

Readings for Future Conflict Studies. Montgomery: Air University, August 1997.

Reagan, Ronald. *Guardian*. (14 Jun 1989) quoted in *The Columbia Dictionary of Quotations* on Microsoft Bookshelf 98 Compact Disk, Document no. X03-08963. (Columbia University Press, 1996).

Rose, Stephen A. (Capt, U.S. Navy). "Information Operations in Joint/Coalition Operations." Briefing for "Legal Aspects of Information Operations Symposium," Maxwell Air Force Base, 20-22 October 1997.

Schwartau, Winn. *Information Warfare*. New York: Thunder's Mouth Press, 1996.

Scorpions. *Live Bites*. Compact Disk #314 526 889-2. Polygram Records, 1995.

Signal. N.p.: n.d. "Information Warfare Strings Trip Wire Warning Strategy."

Spulber, Nicolas. *The American Economy: The Struggle for Supremacy in the 21st Century*. New York: Cambridge University Press, 1995.

Szafranski, Richard. "An Information Warfare SIIOP." In *Information Warfare*, Winn Schwartau, 115-125. New York: Thunder's Mouth Press, 1996.

Thatcher, Margaret. *The Path to Power*. Great Britain: Harper Collins Publishers, 1995.

Toffler, Alvin. *The Third Wave*. New York: Bantam Books, 1980.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War: Making Sense of Today's Global Chaos*. New York: Warner Books, Inc., 1995.

Tzu, Sun. *The Art of War*. Translated by Samuel B. Griffith. New York: Oxford University Press, 1971.

Ullman, Harlan and James Wade, Jr. *Shock and Awe*. Washington, D.C.: GPO, 1996.

United States. Department of the Air Force. *Air Force Doctrine Document 2-5: Information Operations* (4th Draft). Washington, D.C.: 22 July 1997.

United States. Department of the Air Force. *Cornerstones of Information Warfare*. Undated.

United States. Department of the Air Force. *Global Engagement: A Vision for the 21st Century Air Force*. Undated.

United States. Department of the Air Force. "The Use of 'Information Operations' as an Overarching Term." *Staff Summary Sheet*. 26 November 1996.

United States. Joint Chiefs of Staff. *Concept for Future Joint Operations: Part II—Terms and Definitions* on Joint Electronic Library Compact Disk, Washington, D.C.: May 1997.

United States. Joint Chiefs of Staff. *DOD Dictionary*. Joint Pub 1-02. Washington, D.C.: 23 May 1994, Updated through April 1997.

United States. Joint Chiefs of Staff. *Joint Pub 3-13: Joint Doctrine for Information Operations* (2nd Draft). Washington, D.C.: 2 July 1997.

United States. Joint Chiefs of Staff. *Joint Pub 3-13.1: Joint Doctrine for Command and Control Warfare (C2W)*. Washington, D.C.: 7 February 1996.

United States. Joint Chiefs of Staff. *Joint Pub 3-53: Doctrine for Joint Psychological Operations*. Washington, D.C.: 10 July 1996.

United States. Joint Chiefs of Staff. *Joint Vision 2010*. Washington, D.C.: Undated.

United States. Joint Chiefs of Staff. *National Military Strategy of the United States of America 1995*. (1995). In *Joint Electronic Library*, Compact Disk. OC Incorporated, 1997.

United States. President. *A National Security Strategy for a New Century*. Washington: May 1997.

United States. President. Executive Order 13010. "Critical Infrastructure Protection, amended by EO 13025, 13041, and 13064." (15 July 1996), 1-5, on-line, internet www.pccip.gov/eo13010.html.

United States. President's Commission on Critical Infrastructure Protection. *Critical Foundations: Protecting America's Infrastructures, The Report of the President's Commission on Critical Infrastructure Protection, Oct 1997*. Washington, D.C.: October, 1997, on-line, internet http://www.pccip.gov.

United States. President's Commission on Critical Infrastructure Protection. *Critical Foundations: Thinking Differently.* Undated, n.p.: on-line, internet, http://www.pccip.gov.

United States. President's Commission on Critical Infrastructure Protection. *Our Nation's Critical Infrastructures: Working Definitions*. 1997, n.p.; on-line, internet, 10/6/1997, available from http://www.pccip.gov/glossary.html.

United States. President's Commission on Critical Infrastructure Protection. *Overview Briefing*. June, 1997, n.p.: on-line, internet, http://www.pccip.gov.

United States Congress. *United States Statutes at Large, Chapter 263, Sec. 15.* June 18, 1878. Quoted in Winn Schwartau. *Information Warfare*, 47. New York: Thunder's Mouth Press, 1996.

Wriston, Walter B. "Bits, Bytes, and Diplomacy." *Foreign Affairs*, September/October 1997, 172-182.

Air War College
Maxwell AFB, Al 36112